PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 29/06

A1

(11) Internationale Veröffentlichungsnummer: **WO 00/11846**

(43) Internationales Veröffentlichungsdatum: 2. März 2000 (02.03.00)

(21) Internationales Aktenzeichen: PCT/EP99/05550

(22) Internationales Anmeldedatum: 31. Juli 1999 (31.07.99)

(30) Prioritätsdaten:
198 38 253.7 22. August 1998 (22.08.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: INSTITUT FÜR TELEMATIK E.V. [DE/DE]; Bahnhofstrasse 30–32, D–54292 Trier (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: ENGEL, Thomas [DE/DE]; Saarburger Strasse 18, D–54294 Trier (DE). HAFFNER, Ernst–Georg [DE/DE]; Poststrasse 5, D–54413 Gusenburg (DE). MEINEL, Christoph [DE/DE]; Am Hohlweg 16, D–54317 Gusterath (DE).

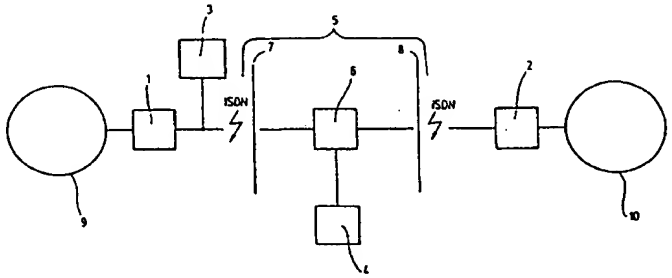
(74) Anwalt: STEIMLE, Josef; Dreiss, Fuhlendorf, Steimle & Becker, Postfach 10 37 62, D–70032 Stuttgart (DE).

(81) Bestimmungsstaaten: CA, CN, JP, KR, RU, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: DATA LINK BETWEEN TWO COMPUTERS AND METHOD FOR TRANSMITTING DATA BETWEEN SAID COMPUTERS

(54) Bezeichnung: DATENVERBINDUNG ZWISCHEN ZWEI RECHNERN UND VERFAHREN ZUR DATENÜBERTRAGUNG ZWISCHEN ZWEI RECHNERN



(57) Abstract

The invention relates to a data link between a first computer (2) and a second computer (2) for transmitting data. The aim of the invention is to provide a data link which is configured in such a way that non authorised third parties are not able to influence said data transmission or to find their way from the outside to one of the computers and to tamper with data. The inventive data link comprises a lock element (6), a first lock gate (7) being placed between said first computer (1) and said lock element (6) and a second lock gate (8) being placed between said second computer (2) and said lock element (6). The first lock gate (7) is closed when the second one (8) is opened and vice–versa.

(57) **Zusammenfassung**

Die vorliegende Erfindung betrifft eine Datenverbindung zwischen einem ersten Rechner (1) und einem zweiten Rechner (2) zum Zwecke der Datenübertragung. Um eine solche Datenverbindung derart auszugestalten, dass es unberechtigten Dritten nicht möglich ist, die Datenübertragung zu beeinflussen oder sich zu einem der Rechner von außen Zugang zu verschaffen und dort die Daten zu manipulieren, schlägt die Erfindung vor, daß in der Datenverbindung ein Schleusenelement (6) angeordnet ist, wobei zwischen dem ersten Rechner (1) und dem Schleusenelement (6) ein erstes Schleusentor (7) und zwischen dem zweiten Rechner (2) und dem Schleusenelement (6) ein zweites Schleusentor (8) angeordnet ist, und wobei das erste Schleusentor (7) geschlossen ist, wenn das zweite Schleusentor (8) geöffnet ist, und umgekehrt, das zweite Schleusentor (8) geschlossen ist, wenn das erste Schleusentor (7) geöffnet ist.

Titel: **Datenverbindung zwischen zwei Rechnern und Verfahren zur Datenübertragung zwischen zwei Rechnern**

Beschreibung

Die vorliegende Erfindung betrifft eine Datenverbindung zwischen einem ersten Rechner und einem zweiten Rechner zum Zwecke der Datenübertragung. Außerdem betrifft sie ein Verfahren zum Übertragen von Daten zwischen einem ersten Rechner zu einem zweiten Rechner über eine Datenverbindung.

Der erste Rechner kann bspw. Teil eines internen unternehmensweiten Rechnernetzwerkes sein. Der zweite Rechner könnte als ein Rechner im weltumspannenden Internet ausgebildet sein.

Jede Datenübertragung zwischen zwei Rechnern wirft Fragen nach der Sicherheit einer solchen Übertragung gegen

unbefugtes Mithören oder gar Manipulieren der Daten oder des Übertragungsvorgangs durch unberechtigte Dritte auf. Für Unternehmen, Banken und Behörden kommt ein weiterer Sicherheitsaspekt hinzu, wenn das eigene unternehmensweite Rechnernetz gegen Angriffe von außerhalb, bspw. aus dem Internet, zu schützen ist. Insbesondere dann, wenn eine aktive Verbindung zwischen Unternehmen und Internet besteht, kann durch unbefugte Zugriffe auf das interne Rechnernetz eines Unternehmens die Datensicherheit in diesem Rechnernetz gefährdet werden.

Aus dem Stand der Technik sind eine Vielzahl von unterschiedlich ausgestalteten Datenverbindungen zur Datenübertragung bekannt. Zur Lösung der Sicherheitsproblematik werden sog. Firewalls eingesetzt. Bei den Firewalls werden die (TCP/IP-) Datenpakete analysiert, unberechtigte Zugriffe verwehrt und berechtigte Anforderungen zugelassen. Die Firewalls stellen jedoch keine physikalische Trennung zwischen dem internen Rechnernetz eines Unternehmens und der Außenwelt her. Durch Manipulation der Firewalls von außerhalb oder durch anderweitig unberechtigten Zugriff ist es deshalb nach wie vor möglich, sich von außerhalb Zugang zu dem internen Rechnernetz zu verschaffen und die Datensicherheit in dem unternehmensweiten Rechnernetz zu gefährden. Wenn die Sicherheitsbedürfnisse eines Unternehmens besonders hoch sind, können die bekannten Firewalls keine ausreichende Sicherheit bieten.

Es ist deshalb die Aufgabe der vorliegenden Erfindung, eine Datenverbindung der eingangs genannten Art dahingehend auszugestalten und weiterzubilden, daß es unberechtigten Dritten nicht möglich ist, sich während einer Datenübertragung durch unberechtigten Zugriff Zugang zu dem ersten Rechner zu verschaffen und dort die Daten zu manipulieren.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von der Datenverbindung der eingangs genannten Art vor, daß in der Datenverbindung ein Schleusenelement angeordnet ist, wobei zwischen dem ersten Rechner und dem Schleusenelement ein erstes Schleusentor (inner flood-gate, IFG) und zwischen dem zweiten Rechner und dem Schleusenelement ein zweites Schleusentor (outer flood-gate, OFG) angeordnet ist(und wobei das erste Schleusentor geschlossen ist, wenn das zweite Schleusentor geöffnet ist und umgekehrt das zweite Schleusentor geschlossen ist, wenn das erste Schleusentor geöffnet ist.

Erfindungsgemäß ist erkannt worden, daß erst durch eine physikalische Trennung der beiden Rechner während der Datenübertragung ein Zugriff auf einen der Rechner von außen durch einen unberechtigten Dritten wirksam und zuverlässig verhindert werden kann.

Durch das Schleusenelement erfolgt eine physikalische Trennung der beiden Rechner voneinander. Zu keinem Zeitpunkt der Datenübertragung sind die beiden Rechner miteinander verbunden, sondern je nach Zustand der Schleusentore findet der Informationsaustausch im Rahmen der Datenübertragung nur jeweils mit einer Seite der Kommunikationspartner statt. Dadurch können mit vergleichsweise geringem Aufwand höchste Sicherheitsvorgaben erfüllt werden.

Das Schleusenelement ist bspw. als ein Rechner ausgebildet. Die erfindungsgemäße Datenverbindung führt zu einer geringen, für einen Anwender kaum bemerkbaren Zeitverzögerung bei der Datenübertragung. Während dieser Zeitverzögerung werden die Schleusentore geöffnet und geschlossen und die zu übertragenden Daten analysiert. Durch eine geeignete Ablaufsteuerung der einzelnen Schritte der Datenübertragung kann die Zeitverzögerung auf ein Minimum reduziert werden.

Gemäß einer vorteilhaften Weiterbildung der Erfindung wird vorgeschlagen, daß der erste Rechner in einem ersten Rechnernetzwerk angeordnet ist. Der erste Rechner ist vorzugsweise als ein Server eines Rechnernetzes und das erste Rechnernetzwerk als ein internes unternehmensweites Rechnernetz ausgebildet. Bei derartigen unternehmensinternen Rechnernetzwerken ist die Datensicherheit besonders wichtig. Viele Unternehmen wickeln inzwischen einen Großteil ihrer Betriebsabläufe komplett elektronisch über ihre internen

Rechnernetze ab. Durch einen unbefugten Zugang zu diesen Rechnernetzen von außerhalb und durch eine Manipulation der darin enthaltenen Daten kann einem Unternehmen sehr großer Schaden erwachsen. Hier sorgt die erfindungsgemäße Datenverbindung für Abhilfe.

Gemäß einer anderen vorteilhaften Weiterbildung der erfindungsgemäßen Datenverbindung wird vorgeschlagen, daß der zweite Rechner in einem zweiten Rechnernetzwerk angeordnet ist. Der zweite Rechner ist vorzugsweise als ein Internet-Server ausgebildet und das zweite Rechnernetzwerk ist das Internet. Die Angriffe von Dritten über das Internet auf an das Internet angeschlossene unternehmensinterne Rechnernetzwerke stellen eine besonders große Gefahr für die Datensicherheit in solchen Unternehmen dar.

Bei der Datenübertragung von einem Rechner eines internen Rechnernetzes zu einem Rechner des Internets ist die Datensicherheit von ganz besonderer Bedeutung, da theoretisch zigmillionen von Internetnutzern unerlaubterweise in das unternehmensinterne Rechnernetz eindringen und dort abgelegte Daten manipulieren könnten. Außerdem sind in dem weltumspannenden und für jedermann zugänglichen Internet eine Vielzahl von sog. Viren und Trojanischen Pferden in Umlauf, die zu einer ernstzunehmenden Gefahr für den Datenbestand eines Unternehmens werden können, wenn sie erst einmal in das interne Rechnernetz des Unternehmens eingedrungen sind. Die

erfindungsgemäße Datenverbindung bietet eine geeignete Plattform, um einen sicheren und zuverlässigen Schutz vor Viren etc. zu gewährleisten. Dazu müssen in der Datenverbindung, vorzugsweise in dem Schleusenelement, geeignete Analysemittel angeordnet werden.

Gemäß einer anderen vorteilhaften Weiterbildung der Erfindung wird vorgeschlagen, daß in dem ersten Rechnernetzwerk ein dritter Rechner und in dem Schleusenelement ein vierter Rechner angeordnet ist.

Der vierte Rechner kann sich innerhalb des Schleusenelements in einer eigenen Netzwerkumgebung befinden, die jedoch physikalisch sowohl von dem ersten Rechnernetzwerk als auch von dem zweiten Rechnernetzwerk getrennt sein muß. Der Sinn des vierten Rechners besteht darin, verschiedene Analyseprozesse innerhalb des Schleusenelements durchzuführen und somit eine gewisse Vorselektion zu treffen.

Zum Senden von Daten werden die zu sendenden Daten von dem ersten Rechner zu dem dritten Rechner gesendet. In dem dritten Rechner werden die Daten analysiert und überprüft. Die Analyse der zu sendenden Daten kann auch auf dem ersten Rechner erfolgen. Erst wenn die Überprüfung keine Beanstandungen ergeben hat, wird das erste Schleusentor geöffnet. Dann werden die Daten von dem dritten Rechner zu dem Schleusenelement gesendet, und anschließend wird das

erste Schleusentor wieder geschlossen. Erst nach vollständigem Schließen des ersten Schleusentors wird das zweite Schleusentor geöffnet. Dann werden die Daten von dem Schleusenelement an den zweiten Rechner gesendet, und danach wird das zweite Schleusentor wieder geschlossen.

Zum Empfangen von Daten wird zunächst das zweite Schleusentor geöffnet und die zu empfangenden Daten werden von dem zweiten Rechner zu dem Schleusenelement gesendet. Dann wird das zweite Schleusentor geschlossen und erst wenn es vollständig geschlossen ist, wird das erste Schleusentor geöffnet. Anschließend werden die Daten von dem Schleusenelement zu dem dritten Rechner gesendet. Dann wird das erste Schleusentor geschlossen und danach analysiert und überprüft der dritte Rechner die Daten. Erst wenn die Überprüfung keine Beanstandungen ergeben hat, werden die Daten von dem dritten Rechner an den ersten Rechner gesendet.

Durch die physikalische Trennung der beiden Rechner bzw. Rechnernetzwerke voneinander werden Online-Angriffe von außen auf einen der Rechner in einem Rechnernetzwerk verhindert und es ist unmöglich, die Analyseprozesse, die in dem dritten Rechner durchgeführt werden, von außen zu manipulieren.

Vorteilhafterweise ist die Verbindung zwischen dem ersten Rechner und dem zweiten Rechner als eine Integrated-Services-Digital-Network (ISDN)-Verbindung nach dem Net-Terminal-

Basis-Adapter (NTBA)-Standard ausgebildet. An diese ISDN-Verbindung wird auch der dritte Rechner angeschlossen. Der vierte Rechner hängt nicht unmittelbar an dem ISDN-NTBA, da er - über ein eigenes Netz - mit dem Schleusenelement verbunden ist.

Auf diese Weise kann die Funktion des Schleusenelements einfach und wirkungsvoll realisiert werden. Eine ISDN-Verbindung nach dem NTBA-Standard weist zwei Datenübertragungskanäle (B-Kanäle) und einen Steuerkanal (D-Kanal) auf. Somit gestattet ein ISDN-NTBA maximal zwei Datenübertragungsverbindungen gleichzeitig. Die Datenverbindung ist so aufgebaut, daß wenn der dritte Rechner zu dem Schleusenelement eine Verbindung zum Zwecke der Datenübertragung aufbaut, hierfür beide B-Kanäle des ISDN-NTBA benötigt werden: Über den einen B-Kanal erfolgt die Anwahl des Schleusenelements, und über den anderen B-Kanal wird die Datenübertragungsverbindung zu dem Schleusenelement hergestellt (erstes Schleusentor geöffnet). Eine gleichzeitige Verbindung des Schleusenelements zu dem zweiten Rechner ist also ausgeschlossen, da der ISDN-NTBA keinen freien B-Kanal mehr zur Verfügung hat (zweites Schleusentor kann nicht geöffnet werden).

Wenn umgekehrt über einen der beiden B-Kanäle bereits eine Verbindung zwischen dem zweiten Rechner und dem Schleusenelement besteht (zweites Schleusentor geöffnet),

kann der dritte Rechner keine Verbindung mehr zu dem Schleusenelement herstellen (erstes Schleusentor kann nicht geöffnet werden), da dazu, wie oben erläutert, beide B-Kanäle des ISDN-NTBA benötigt werden. Durch die doppelte Verwendung desselben NTBA, einerseits an dem dritten Rechner und andererseits an dem Schleusenelement, kann die Schleusenfunktion der erfindungsgemäßen Datenverbindung auf einfache Weise realisiert werden.

Eine weitere Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren der eingangs genannten Art dahingehend auszugestalten und weiterzubilden, daß es unberechtigten Dritten nicht möglich ist, die Datenübertragung zu beeinflussen oder sich zu einem der Rechner Zugang zu verschaffen und dort die Daten zu manipulieren.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von dem Verfahren der eingangs genannten Art vor, daß die Daten von dem ersten Rechner über ein geöffnetes erstes Schleusentor in ein Schleusenelement übertragen werden, das erste Schleusentor geschlossen und dann ein zweites Schleusentor geöffnet wird und die Daten über das geöffnete zweite Schleusentor zu dem zweiten Rechner und in der entgegengesetzten Richtung in umgekehrter Reihenfolge übertragen werden.

Vorzugsweise werden die Daten von dem ersten Rechner über einen dritten Rechner, der mit dem ersten Rechner in einem gemeinsamen Rechnernetzwerk angeordnet ist, und über das Schleusenelement an den zweiten Rechner und umgekehrt übertragen.

Vorteilhafterweise werden zum Aufbau einer Datenverbindung und zur Datenübertragung zwischen dem dritten Rechner und dem Schleusenelement beide B-Kanäle einer ISDN-Verbindung nach dem Net-Terminal-Basis-Adapter (NTBA)-Standerd verwendet. Dadurch kann die Funktion des Schleusenelements auf einfache und wirkungsvolle Weise realisiert werden.

Gemäß einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, daß in dem dritten Rechner eine Analyse der zu übertragenden Daten durchgeführt wird. Vorzugsweise erfolgt die Analyse nach semantischen Gesichtspunkten.

Der dritte Rechner steht zu keinem Zeitpunkt der Datenübertragung mit dem zweiten Rechnernetzwerk bzw. mit dem zweiten Rechner in direktem Kontakt. Dies wird durch die Schleusentore verhindert, die während der Datenübertragung niemals beide gleichzeitig geöffnet sind. Somit ist es unberechtigten Drittan nicht möglich, während einer Datenübertragung einen direkten Zugriff auf den dritten

Rechner zu erhalten und den in dem dritten Rechner enthaltenen Analysemechanismus zu manipulieren.

In dem Schleusenelement selbst findet dagegen keine Analyse der zu übermittelnden Daten statt, da das Schleusenelement zur Übermittlung von Daten für eine bestimmte Zeitdauer in direktem Kontakt mit dem zweiten Rechnernetzwerk bzw. mit dem zweiten Rechner steht. Während dieser Zeitdauer könnte ein in dem Schleusenelement enthaltener Analysemechanismus durch unberechtigte Dritte manipuliert werden.

Wenn die Daten über das geöffnete erste Schleusentor von dem Schleusenelement zu dem dritten Rechner gesendet werden, können zwar infizierte Dateien, d. h. Dateien, die Viren oder Trojanische Pferde enthalten, in dem dritten Rechner abgelegt werden. Dennoch besteht hier ein entscheidender Unterschied zu der Funktionsweise der bekannten Firewalls. Anstatt online alle Analyseprozesse durchzuführen, kann der dritte Rechner ohne Bedrohung durch einen Zugriff von außen und interaktive Manipulation die passiven Daten, die das Schleusenelement aus dem zweiten Rechnernetzwerk erhalten hat, je nach gewünschter skalierbarer Analysetiefe und Analysedauer untersuchen und ggf. vernichten.

Im Rahmen der semantischen Analyse der Daten kann überprüft werden, ob der Inhalt bestimmter Dateien das unternehmensweite Rechnernetzwerk verlassen und nach außen

gelangen darf. Bei der semantischen Analyse von Dateien werden insbesondere die Anlagen zu elektronischen Nachrichten (eMails) überprüft, da hierüber Dokumente beliebigen Typs versendet werden können. Eine semantische Analyse ist bei dem erfindungsgemäßen Verfahren möglich, da die Analysezeiträume flexibel gestaltet werden können.

Vorzugsweise erfolgt das Senden von Daten von dem ersten Rechner zu dem zweiten Rechner in den nachfolgenden Schritten:

- Die zu sendenden Daten werden von dem ersten Rechner zu dem dritten Rechner gesendet.
- Der dritte Rechner analysiert und überprüft die Daten.
- Das erste Schleusentor wird geöffnet.
- Die Daten werden von dem dritten Rechner (INS) zu dem Schleusenelement gesendet.
- Das erste Schleusentor wird geschlossen.
- Das zweite Schleusentor wird geöffnet.
- Die Daten werden von dem Schleusenelement an den zweiten Rechner gesendet.
- Und das zweite Schleusentor wird geschlossen.

Vorzugsweise erfolgt das Empfangen von Daten von dem zweiten Rechner durch den ersten Rechner in den nachfolgenden Schritten:

- Das zweite Schleusentor wird geöffnet.

- Die zu empfangenden Daten werden von dem zweiten Rechner zu dem Schleusenelement gesendet.
- das zweite Schleusentor wird geschlossen.
- Das erste Schleusentor wird geöffnet.
- Die Daten werden von dem Schleusenelement zu dem dritten Rechner gesendet.
- Das erste Schleusentor wird geschlossen.
- Der dritte Rechner analysiert und überprüft die Daten.
- Und die Daten werden von dem dritten Rechner an den ersten Rechner gesendet.

Das erste Schleusentor wird bevorzugt von dem dritten Rechner angesteuert, das zweite Schleusentor von dem Schleusenelement.

Gemäß einer vorteilhaften Weiterbildung des erfindungsgemäßen Verfahrens werden die zu empfangenden Daten von dem Schleusenelement zu dem dritten Rechner zu dem Zeitpunkt gesendet, zu dem auch die zu sendenden Daten von dem dritten Rechner zu dem Schleusenelement gesendet werden. Dadurch können in einem Zeitschritt zwei unterschiedliche Schritte der Datenübertragung durchgeführt werden. Voraussetzung dafür ist, daß zu diesem Zeitpunkt die Positonen der Schleusentore gleich sind. Im Fall dieser Weiterbildung ist das erste Schleusentor nämlich geöffnet und das zweite Schleusentor geschlossen.

Gemäß einer anderen vorteilhaften Weiterbildung der Erfindung werden die zu empfangenden Daten von dem zweiten Rechner zu dem Schleusenelement zu dem Zeitpunkt gesendet, zu dem auch die zu sendenden Daten von dem Schleusenelement zu dem zweiten Rechner gesendet werden. Zu diesem Zeitpunkt sind das erste Schleusentor geschlossen und das zweite Schleusentor geöffnet.

Gemäß noch einer anderen Weiterbildung des erfindungsgemäßen Verfahrens wird die Analyse der empfangenen Daten zeitgleich mit der Analyse der zu sendenden Daten durchgeführt. Die Analyse der Daten erfolgt vorzugsweise in dem dritten und/oder in dem vierten Rechner. Die Analyse der zu sendenden Daten kann aber auch in dem ersten Rechner erfolgen.

Grundsätzlich ist es möglich jeweils diejenigen Schritte einer Datenübertragung in einem Zeitschritt durchzuführen, bei denen die Position der Schleusentore gleich ist.

Ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung wird im Folgenden anhand der Zeichnung näher erläutert. Es zeigt:

Fig. 1 eine erfindungsgemäße Datenverbindung.

In Figur 1 ist eine Datenverbindung zwischen einem ersten Rechner 1 und einem zweiten Rechner 2 zum Zwecke der

Datenübertragung dargestellt. In der Datenverbindung ist ein Schleusenelement 6 angeordnet, wobei zwischen dem ersten Rechner 1 und dem Schleusenelement 6 ein erstes Schleusentor 7 und zwischen dem zweiten Rechner 2 und dem Schleusenelement 6 ein zweites Schleusentor 8 angeordnet ist. Das erste Schleusentor 7 ist geschlossen, wenn das zweite Schleusentor 8 geöffnet ist, und umgekehrt ist das zweite Schleusentor 8 geschlossen, wenn das erste Schleusentor 7 geöffnet ist.

Der erste Rechner 1 ist in einem ersten Rechnernetzwerk 9 angeordnet, wobei der erste Rechner 1 als ein Server eines Rechnernetzes und das erste Rechnernetzwerk 9 als ein internes unternehmensweites Rechnernetz ausgebildet ist. Der zweite Rechner 2 ist in einem zweiten Rechnernetzwerk 10 angeordnet, wobei der zweite Rechner 2 als ein Internet-Server ausgebildet ist und das zweite Rechnernetzwerk 10 das Internet ist. In dem ersten Rechnernetzwerk 9 ist ein dritter Rechner 3 und in dem Schleusenelement 6 ein vierter Rechner 4 angeordnet. Der Sinn des vierten Rechners 4 besteht darin, verschiedene Analyseprozesse innerhalb des Schleusenelements 6 durchzuführen und somit eine gewisse Vorselektion zu treffen.

Um nun Daten von dem ersten Rechner 1 zu dem zweiten Rechner 2 zu senden, werden die zu sendenden Daten zunächst von dem ersten Rechner 1 zu dem dritten Rechner 3 gesendet. In dem dritten Rechner 3 werden die Daten analysiert und überprüft.

Die Analyse erfolgt vorzugsweise nach semantischen Gesichtspunkten. Erst wenn die Analyse keine Beanstandungen ergeben hat, wird das erste Schleusentor 7 geöffnet. Dann werden die Daten von dem dritten Rechner 3 zu dem Schleusenelement 6 gesendet, und anschließend wird das erste Schleusentor 7 wieder geschlossen. Erst nach vollständigem Schließen des ersten Schleusentors 7 wird das zweite Schleusentor 8 geöffnet. Dann werden die Daten von dem Schleusenelement 6 an den zweiten Rechner 2 gesendet, und danach wird das zweite Schleusentor 8 wieder geschlossen.

Zum Empfangen von Daten von dem zweiten Rechner 2 durch den ersten Rechner 1 wird zunächst das zweite Schleusentor 8 geöffnet und die zu empfangenden Daten werden von dem zweiten Rechner 2 zu dem Schleusenelement 6 gesendet. Dann wird das zweite Schleusentor 8 geschlossen, und erst wenn es vollständig geschlossen ist, wird das erste Schleusentor 7 geöffnet. Anschließend werden die Daten von dem Schleusenelement 6 zu dem dritten Rechner 3 gesendet. Dann wird das erste Schleusentor 7 geschlossen. Danach analysiert und überprüft der dritte Rechner 3 die Daten. Erst wenn die Analyse keine Beanstandungen ergeben hat, werden die Daten von dem dritten Rechner 3 an den ersten Rechner 1 gesendet.

Durch das Schleusenelement 6 zwischen dem ersten Rechner 1 und dem zweiten Rechner 2 erfolgt eine physikalische Trennung der beiden Rechner 1, 2 bzw. der beiden Rechnernetzwerke 9,

10. Dadurch können Online-Angriffe von außen auf den ersten Rechner 1 in dem Rechnernetzwerk 9 verhindert werden, und es ist unmöglich, die Analyseprozesse, die in dem dritten Rechner 3 durchgeführt werden, von außen zu manipulieren, da ein direkter Zugriff von außen auf den dritten Rechner 3 dank des Schleusenelements 6 nicht möglich ist.

Die Datenverbindung zwischen dem ersten Rechner 1 und dem zweiten Rechner 2 ist als eine Integrated-Services-Digital-Network (ISDN)-Verbindung 5 nach dem Net-Terminal-Basis-Adapter (NTBA)-Standard ausgebildet. An die ISDN-Verbindung 5 ist auch der dritter Rechner 3 angeschlossen. Der vierte Rechner 4 hängt nicht unmittelbar an dem ISDN-NTBA, da er - über ein eigenes Netz - mit dem Schleusenelement 6 verbunden ist. Auf diese Weise kann die Funktion des Schleusenelements 6 einfach und wirkungsvoll realisiert werden. die ISDN-Verbindung 5 nach dem NTBA-Standard weist zwei Datenübertragungskanäle (B-Kanäle) und einen Steuerkanal (D-Kanal) auf. Somit gestattet ein ISDN-NTBA maximal zwei Datenübertragungsverbindungen gleichzeitig.

Wenn der dritte Rechner 3 zu dem Schleusenelement 6 eine Verbindung zum Zwecke der Datenübertragung aufbaut, werden hierfür beide B-Kanäle benötigt: Über den einen B-Kanal erfolgt die Anwahl des Schleusenelements 6, und über den anderen B-Kanal wird die Datenübertragungsverbindung zu dem Schleusenelement 6 hergestellt. Die zwischen dem dritten

Rechner 3 und dem Schleusenelement 6 hergestellte ISDN-Verbindung 5 entspricht einer Schleusentorstellung, bei der das erste Schleusentor 7 geöffnet und das zweite Schleusentor 8 geschlossen ist. Eine gleichzeitige Verbindung des Schleusenelements 6 zu dem zweiten Rechner 2 (zweites Schleusentor 8 geöffnet) ist also aufgrund der technischen Gegebenheiten bei ISDN-NTBAs ausgeschlossen.

Wenn umgekehrt über einen der beiden B-Kanäle bereits eine Verbindung zwischen dem zweiten Rechner 2 in dem zweiten Rechnernetzwerk 10 und dem Schleusenelement 6 besteht (zweites Schleusentor 8 geöffnet), kann der dritte Rechner 3 keine Verbindung mehr zu dem Schleusenelement 6 herstellen (erstes Schleusentor 7 kann nicht geöffnet werden), da dazu, wie oben erläutert, beide B-Kanäle des ISDN-NTBA benötigt werden.

Patentansprüche

1. Datenverbindung zwischen einem ersten Rechner (1) und einem zweiten Rechner (2) zum Zwecke der Datenübertragung, **dadurch gekennzeichnet**, daß in der Datenverbindung ein Schleusenelement (6) angeordnet ist, wobei zwischen dem ersten Rechner (1) und dem Schleusenelement (6) ein erstes Schleusentor (7) und zwischen dem zweiten Rechner (2) und dem Schleusenelement (6) ein zweites Schleusentor (8) angeordnet ist, und wobei das erste Schleusentor (7) geschlossen ist, wenn das zweite Schleusentor (8) geöffnet ist und umgekehrt das zweite Schleusentor (8) geschlossen ist, wenn das erste Schleusentor (7) geöffnet ist.

2. Datenverbindung nach Anspruch 1, dadurch gekennzeichnet, daß der erste Rechner (1) in einem ersten Rechnernetzwerk (9) angeordnet ist.

3. Datenverbindung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der zweite Rechner (2) in einem zweiten Rechnernetzwerk (10) angeordnet ist.

4. Datenverbindung nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß der erste Rechner (1) als ein Server eines Rechnernetzes und das erste Rechnernetzwerk (9)

als ein internes unternehmensweites Rechnernetz ausgebildet ist.

5. Datenverbindung nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß der zweite Rechner (2) als ein Internet-Server ausgebildet ist und das zweite Rechnernetzwerk (10) das Internet ist.

6. Datenverbindung nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß in dem ersten Rechnernetzwerk (9) ein dritter Rechner (3) und in dem Schleusenelement (6) ein vierter Rechner (4) angeordnet ist.

7. Datenverbindung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Verbindung zwischen dem ersten Rechner (1) und dem zweiten Rechner (2) als eine Integrated-Services-Digital-Network (ISDN)-Verbindung nach dem Net-Terminal-Basis-Adapter (NTBA)-Standard ausgebildet ist.

8. Verfahren zum Übertragen von Daten zwischen einem ersten Rechner (1) zu einem zweiten Rechner (2) über eine Datenverbindung, **dadurch gekennzeichnet**, daß die Daten in der einen Richtung von dem ersten Rechner (1) über ein geöffnetes erstes Schleusentor (7) in ein Schleusenelement (6) übertragen werden, das erste Schleusentor (7) geschlossen und dann ein zweites

Schleusentor (8) geöffnet wird und die Daten über das geöffnete zweite Schleusentor (8) zu dem zweiten Rechner (2) und in der entgegengesetzten Richtung in umgekehrter Reihenfolge übertragen werden.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Daten von dem ersten Rechner (1) über einen dritten Rechner (3), der mit dem ersten Rechner (1) in einem gemeinsamen Rechnernetzwerk (7) angeordnet ist, und über das Schleusenelement (6) an den zweiten Rechner (2) und umgekehrt übertragen werden.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß zum Aufbau einer Datenverbindung und zur Datenübertragung zwischen dem dritten Rechner (3) und dem Schleusenelement (6) beide B-Kanäle einer ISDN-Verbindung nach dem Net-Terminal-Basis-Adapter (NTBA)-Standard verwendet werden.

11. Verfahren nach Anspruch 9 oder 10, dadurch gekennzeichnet, daß in dem dritten Rechner (3) eine Analyse der zu übertragenden Daten durchgeführt wird.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß die Analyse nach semantischen Gesichtspunkten erfolgt.

13. Verfahren nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß die Tiefe und die Dauer der Analyse individuell eingestellt werden.

14. Verfahren nach einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, daß zum Senden von Daten
- die zu sendenden Daten von dem ersten Rechner (1) zu dem dritten Rechner (3) gesendet werden,
- der dritte Rechner (3) die Daten analysiert und überprüft,
- das erste Schleusentor (7) geöffnet wird,
- die Daten von dem dritten Rechner (3) zu dem Schleusenelement (6) gesendet werden,
- das erste Schleusentor (7) geschlossen wird,
- das zweite Schleusentor (8) geöffnet wird,
- die Daten von dem Schleusentor (6) an den zweiten Rechner (2) gesendet werden, und
- das zweite Schleusentor (8) geschlossen wird.

15. Verfahren nach einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, daß zum Empfangen von Daten
- das zweite Schleusentor (8) geöffnet wird,
- die zu empfangenden Daten von dem zweiten Rechner (2) zu dem Schleusenelement (6) gesendet werden,
- das zweite Schleusentor (8) geschlossen wird,
- das erste Schleusentor (7) geöffnet wird,

- die Daten von dem Schleusenelement (6) zu dem dritten Rechner (3) gesendet werden,
- das erste Schleusentor (7) geschlossen wird,
- der dritte Rechner (3) die Daten analysiert und überprüft, und
- die Daten von dem dritten Rechner (3) an den ersten Rechner (1) gesendet werden.

16. Verfahren nach Anspruch 14 oder 15, dadurch gekennzeichnet, daß die zu empfangenden Daten von dem Schleusenelement (6) zu dem dritten Rechner (3) zu dem Zeitpunkt gesendet werden, zu dem auch die zu sendenden Daten von dem dritten Rechner (3) zu dem Schleusenelement (6) gesendet werden.

17. Verfahren nach einem der Ansprüche 14 bis 16, dadurch gekennzeichnet, daß die zu empfangenden Daten von dem zweiten Rechner (2) zu dem Schleusenelement (6) zu dem Zeitpunkt gesendet werden, zu dem auch die zu sendenden Daten von dem Schleusenelement (6) zu dem zweiten Rechner (2) gesendet werden.

18. Verfahren nach einem der Ansprüche 14 bis 17, dadurch gekennzeichnet, daß die Analyse der empfangenen Daten zeitgleich mit der Analyse der zu sendenden Daten durchgeführt wird.

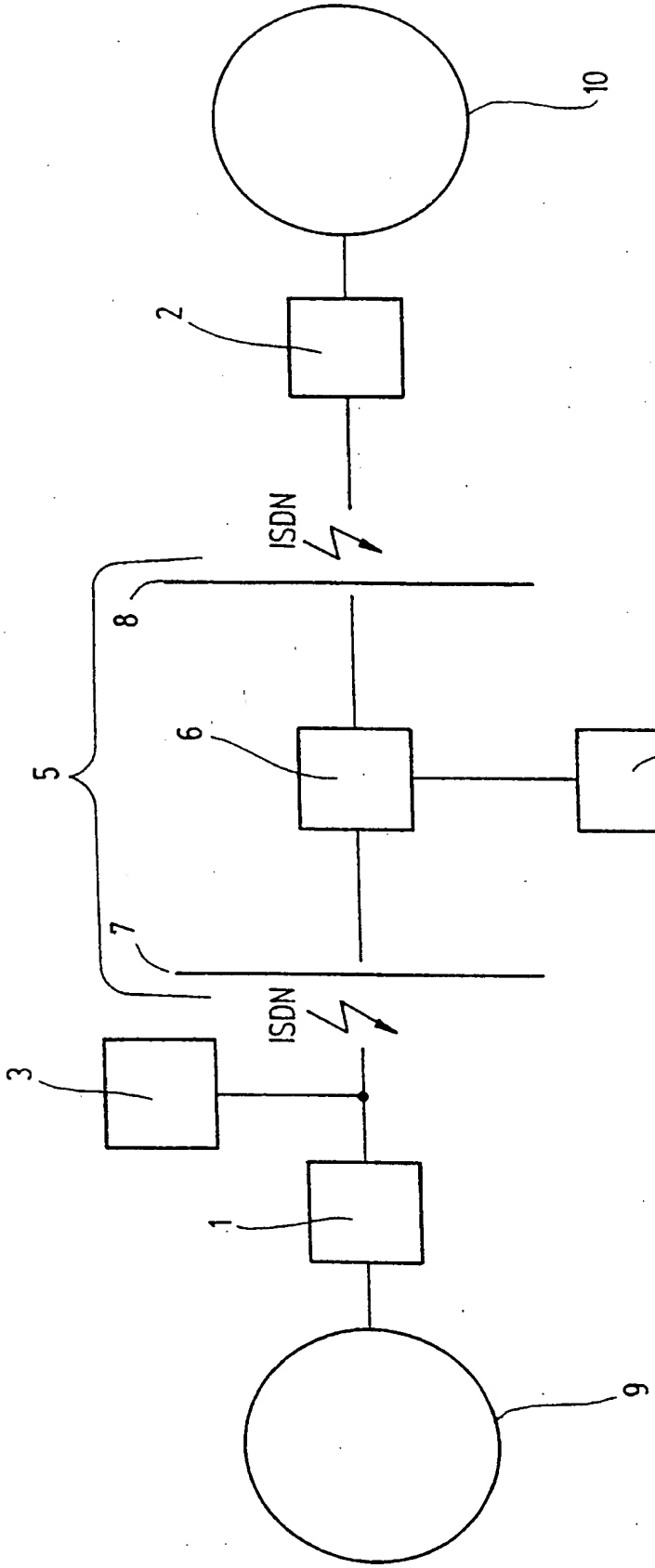


Fig.1

INTERNATIONALER RECHERCHENBERICHT

Intern: ales Aktenzeichen
PCT/EP 99/05550

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L29/06

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	POHLMANN N: "FIREWALL-SYSTEME" FUNKSCHAU,DE,FRANZIS-VERLAG K.G. MUNCHEN, Bd. 71, Nr. 17, Seite 63-67 XP000847738 ISSN: 0016-2841 das ganze Dokument ---	1-18
A	HORNAUER G: "ISDN-FIREWALL MEHR SICHERHEIT FUER ISDN-TK ANLAGEN" NET - ZEITSCHRIFT FUER KOMMUNIKATIONSMANAGEMENT,DE,HUTHIG VERLAG, HEILDERBERG, Bd. 52, Nr. 3, Seite 62-63 XP000740479 ISSN: 0947-4765 das ganze Dokument -----	1-18

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
24. Januar 2000	02/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

1

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/EP 99/05550

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	POHLMANN N: "FIREWALL-SYSTEME" FUNKSCHAU,DE,FRANZIS-VERLAG K.G. MUNCHEN, vol. 71, no. 17, page 63-67 XP000847738 ISSN: 0016-2841 the whole document ---	1-18
A	HORNAUER G: "ISDN-FIREWALL MEHR SICHERHEIT FUER ISDN-TK ANLAGEN" NET - ZEITSCHRIFT FUER KOMMUNIKATIONSMANAGEMENT,DE,HUTHIG VERLAG, HEILDERBERG, vol. 52, no. 3, page 62-63 XP000740479 ISSN: 0947-4765 the whole document -----	1-18

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 January 2000	02/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Adkhis, F